WHAT IS CLAIMED IS:

1.   A method of collecting, storing and processing usage data from a device, comprising:

5   (a) extracting the usage data from the device, wherein the usage data is associated with a customer identifier;

(b) obfuscating, but not eliminating, the customer identifier from the extracted usage data; and

(c) correlating the extracted usage data over a period of time using the obfuscated

10   customer identifier.

2.   The method of claim 1, wherein the usage data is processed in accordance with a privacy policy recorded for each customer.

15   3.   The method of claim 1, wherein both the customer identifier and the usage data are stored for "opt-in" customers.

4.   The method of claim 1, wherein only the obfuscated customer identifier and the usage data are stored for "opt-neutral" customers.

20

5.   The method of claim 1, wherein neither the customer identifier nor the usage data are stored for "opt-out" customers.

6.   The method of claim 1, wherein the obfuscating step is performed only for

25   extracted usage data associated with an "opt-neutral" customer.

7.   The method of claim 1, wherein the obfuscating step comprises creating a replacement identifier for the customer identifier from the extracted usage data.

8.   The method of claim 7, wherein the obfuscating step comprises translating the customer identifier from the extracted usage data into the replacement identifier.

9.   The method of claim 8, wherein the translating step comprises performing a translation function that produces a unique replacement identifier for every customer identifier.

10.   The method of claim 8, wherein the translating step comprises performing a translation function that produces a non-unique replacement identifier for every customer identifier.

11.   The method of claim 1, wherein the translating step comprises performing a one-way translation function that has an inverse function that is difficult to perform.

12.   The method of claim 1, wherein the device sends the viewing usage data along with a usage identifier that is independent of the customer identifier.

13.   The method of claim 12, wherein the obfuscating step comprises translating the customer identifier from the extracted usage data into a replacement identifier using the usage identifier.

14.   An apparatus for collecting, storing and processing usage data from a device, comprising:

(a) means for extracting the usage data from the device, wherein the usage data is associated with a customer identifier;

(b) means for obfuscating, but not eliminating, the customer identifier from the extracted usage data; and

(c) means for correlating the extracted usage data over a period of time using the obfuscated customer identifier.

15.   The apparatus of claim 14, wherein the usage data is processed in accordance with a privacy policy recorded for each customer.

16.   The apparatus of claim 14, wherein both the customer identifier and the usage data are stored for "opt-in" customers.

17.   The apparatus of claim 14, wherein only the obfuscated customer identifier and the usage data are stored for "opt-neutral" customers.

18.   The apparatus of claim 14, wherein neither the customer identifier nor the usage data are stored for "opt-out" customers.

19.   The apparatus of claim 14, wherein the means for obfuscating is performed only for extracted usage data associated with an "opt-neutral" customer.

20.   The apparatus of claim 14, wherein the means for obfuscating comprises means for creating a replacement identifier for the customer identifier from the extracted usage data.

21.   The apparatus of claim 20, wherein the means for obfuscating comprises means for translating the customer identifier from the extracted usage data into the replacement identifier.

22.   The apparatus of claim 21, wherein the means for translating comprises means for performing a translation function that produces a unique replacement identifier for every customer identifier.

23.   The apparatus of claim 21, wherein the means for translating comprises means for performing a translation function that produces a non-unique replacement identifier for every customer identifier.

24.   The apparatus of claim 14, wherein the means for translating comprises means for performing a one-way translation function that has an inverse function that is difficult to perform.

5

25.   The apparatus of claim 14, wherein the device sends the viewing usage data along with a usage identifier that is independent of the customer identifier.

26.   The apparatus of claim 25, wherein the means for obfuscating comprises

10   means for translating the customer identifier from the extracted usage data into a replacement identifier using the usage identifier.

27.   An article of manufacture embodying logic for collecting, storing and processing usage data from a device, the logic comprising:

15   (a) extracting the usage data from the device, wherein the usage data is associated with a customer identifier;

(b) obfuscating, but not eliminating, the customer identifier from the extracted usage data; and

(c) correlating the extracted usage data over a period of time using the obfuscated

20   customer identifier.

28.   The article of claim 27, wherein the usage data is processed in accordance with a privacy policy recorded for each customer.

25   29.   The article of claim 27, wherein both the customer identifier and the usage data are stored for "opt-in" customers.

30.   The article of claim 27, wherein only the obfuscated customer identifier and the usage data are stored for "opt-neutral" customers.

30

31.   The article of claim 27, wherein neither the customer identifier nor the usage data are stored for "opt-out" customers.

32.   The article of claim 27, wherein the obfuscating step is performed only for extracted usage data associated with an "opt-neutral" customer.

33.   The article of claim 27, wherein the obfuscating step comprises creating a replacement identifier for the customer identifier from the extracted usage data.

34.   The article of claim 33, wherein the obfuscating step comprises translating the customer identifier from the extracted usage data into the replacement identifier.

35.   The article of claim 34, wherein the translating step comprises performing a translation function that produces a unique replacement identifier for every customer identifier.

36.   The article of claim 34, wherein the translating step comprises performing a translation function that produces a non-unique replacement identifier for every customer identifier.

37.   The article of claim 27, wherein the translating step comprises performing a one-way translation function that has an inverse function that is difficult to perform.

38.   The article of claim 27, wherein the device sends the viewing usage data along with a usage identifier that is independent of the customer identifier.

39.   The article of claim 38, wherein the obfuscating step comprises translating the customer identifier from the extracted usage data into a replacement identifier using the usage identifier.